AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America
v.
PARKER WILLIAM WHITE

Case No. 2:23-mj-00817-DUTY

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of February 21, 2023 in the county of Los Angeles in the Central District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 1470	Transfer of Obscene Material to a Minor

This criminal complaint is based on these facts:

See attached affidavit

☑ Continued on the attached sheet.

/s/
Complainant's signature

DACID SA Michael Charlton
Printed name and title

Sworn to before me and signed in my presence.

Date: 2/21/23

Judge's signature

City and state: Los Angeles

Hon. Margo A. Rocconi
Printed name and title

AUSA: L. Allsop x3165

AFFIDAVIT

I, Michael J. Charlton, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Department of the Army Criminal Investigation Division ("DACID") and have been so employed since November of 2021.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of a criminal complaint against, and arrest warrant for PARKER WILLIAM WHITE ("WHITE"), a private in the United States Army, presently stationed at a military base in Fort Irwin, California, for a violation of 18 U.S.C. § 1470 (Transfer of Obscene Material to a Minor).

3. This affidavit is also made in support of applications for warrants to search a Black iPhone SE, Model MMX53LL/A, bearing IMEI No. 350472506112686, and bearing Serial No. NMMW69595K ("SUBJECT DEVICE 1"); and a Black/Grey iPhone 12 Pro Max, Model MG923LL/A, bearing IMEI No. 354876506002091, and bearing Serial No. F2LF69170D43 ("SUBJECT DEVICE 2") (collectively, the "SUBJECT DEVICES") as described more fully in Attachment A-1; and the person of WHITE as described more fully in Attachment A-2. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities for violations of 18 U.S.C. § 2251 (Sexual Exploitation of Children); 18 U.S.C. § 2252A (Certain Activities Relating to Material Constituting or Containing Child Pornography); 18

U.S.C. § 2422(b) (Coercion and Enticement of a Minor to Engage in Criminal Sexual Activity); and 18 U.S.C. § 1470 (Transfer of Obscene Material to a Minor) (the "SUBJECT OFFENSES"), as described more fully in Attachment B. Attachments A-1, A-2, and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest warrant, and search warrants and does not purport to set forth all my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only. All dates and times are approximate.

III. BACKGROUND OF SPECIAL AGENT MICHAEL J. CHARLTON

5. I am employed as a Special Agent with the DACID in Fort Irwin, California, and I have been employed since November 2021. As a Special Agent, I have investigated a variety of criminal offenses including, but not limited to child assault; sexual assault; domestic violence; possessing, receiving, or viewing child pornography; and consumption of drugs. In the course of my employment with the DACID, I have received an extensive four-month training course in conducting criminal investigations and additional advanced training in domestic violence and sexual assault investigations. I am responsible for the investigation of certain felony crimes where a United

States Army nexus exists. In addition, as a Federal Agent of the United States, I am authorized to investigate crimes involving violations of the Uniform Code of Military Justice (10 U.S.C. § 47, hereinafter "UCMJ"), U.S. Criminal Code (18 U.S.C.), and other federal and state laws where there is a United States Army or Department of Defense interest.

IV. SUMMARY OF PROBABLE CAUSE

6. On or about January 27, 2022, DACID received a phone call from Bay County Sheriff's Office, which is in Panama City, Florida, regarding a United States Army private who was stationed at Fort Irwin in California (WHITE). According to a sheriff's deputy, WHITE, then a 21-year-old-man, had been engaging in a sexual relationship with a 14-year-old (E.V.G.), who lived in Florida. During a forensic interview, E.V.G. stated that WHITE knew that s/he was 14 years old, and when they first began talking via Instagram, he had presented himself as a 15-year-old boy. During the forensic interview, the sheriff's deputy, acting in an undercover capacity and as E.V.G., used E.V.G.'s phone to communicate with WHITE via Snapchat, and during their conversation, WHITE sent photographs of his penis and videos of him masturbating while wearing what appeared to be a United States Army uniform.

7. After receiving this information from the sheriff's deputy, on that same date, DACID conducted a recorded, Mirandized interview of WHITE. During the interview, WHITE admitted to being in a relationship with E.V.G. knowing that she was only 14 years old, and to also being in relationships with

other individuals who he believed were minors. WHITE also admitted to having a video of E.V.G. on his phone that showed him/her masturbating with a brush. WHITE insisted that he had saved the video accidentally. WHITE also admitted to sending E.V.G. photographs of his genitals and videos of him masturbating. Pursuant to Magistrate Authorization, DACID seized and reviewed WHITE's cellphone (SUBJECT DEVICE 1) and discovered approximately 27 photographs and videos of suspected minors either nude, semi-nude, or engaging in sexually explicit acts.

8. On or about June 7, 2022, DACID conducted a second, recorded, Mirandized interview of WHITE. During the interview, WHITE admitted to continuing to engage in relationships with suspected minors, and he also admitted to getting a new cellphone (SUBJECT DEVICE 2) and syncing it to his iCloud, where he had stored the photographs and videos of suspected minors nude, semi-nude, and engaging in sexually explicit acts. By syncing SUBJECT DEVICE 2 with his iCloud, WHITE was able to regain access to the sexually explicit videos and photographs on SUBJECT DEVICE 1, which DACID had previously seized. During the interview, WHITE boasted that it was "not that fucking hard" for him to get access to these videos and photographs. Pursuant to Magistrate Authorization, DACID seized and reviewed WHITE's cellphone (SUBJECT DEVICE 2). DACID found the same sexually explicit photographs and videos on SUBJECT DEVICE 2 that were on SUBJECT DEVICE 1. DACID did not find any new photographs or

videos containing suspected child pornography on SUBJECT DEVICE 2.

9. In addition to E.V.G., DACID has identified five other minors that, using text message, Snapchat, and other social media platforms, WHITE has engaged in relationships with.

V. BACKGROUND ON CHILD EXPLOITATION OFFENSES, COMPUTERS, THE INTERNET, AND DEFINITION OF TERMS

10. In this affidavit, the terms "minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined as set forth in 18 U.S.C. § 2256. The term "computer" is defined as set forth in 18 U.S.C. § 1030(e)(1).

11. Based upon my training and experience investigating offenses related to child pornography, and information related to me by other law enforcement officers involved in the investigation of child pornography, I know the following information about the use of computers with child pornography:

a. Computers and Child Pornography. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. Child pornographers can now produce both still and moving images directly from a common video camera and can convert these images into computer-readable formats. The use of digital technology has enabled child pornographers to electronically receive, distribute, and possess large numbers of child exploitation images and videos with other Internet users worldwide.

b. File Storage. Computer users can choose their method of storing files: either on a computer's hard drive, an external hard drive, a memory card, a Universal Serial Bus ("USB") thumb drive, a smart phone, or other digital media device, etc. (i.e., "locally") or on virtual servers accessible from any digital device with an Internet connection (i.e., "cloud storage"). Computer users frequently transfer files from one location to another, such as from a phone to a computer or from cloud storage to an external hard drive. Computer users also often create "backup," or duplicate, copies of their files. In this way, digital child pornography is extremely mobile and such digital files are easily reproduced and transported. For example, with the click of a button, images and videos containing child pornography can be put onto external hard drives small enough to fit onto a keychain. Just as easily, these files can be copied onto compact disks and/or stored on mobile digital devices, such as smart phones and tablets. Furthermore, even if the actual child pornography files are stored on a "cloud," files stored in this manner can only be accessed via a digital device. Therefore, viewing this child pornography would require a computer, smartphone, tablet, or some other digital device that allows the user to access and view files on the Internet.

c. Internet. The term "Internet" is defined as the worldwide network of computers -- a noncommercial, self-governing network devoted mostly to communication and research with roughly 500 million users worldwide. The Internet is not

an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. To access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider ("ISP"), which operates a host computer with direct access to the Internet.

d. Internet Service Providers. Individuals and businesses obtain access to the Internet through ISPs. ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customer's behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format.

e. IP Addresses. An Internet Protocol address ("IP Address") is a unique numeric address used to connect to the Internet. An IPv4 IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). In simple terms, one computer in a home may connect directly to

the Internet with an IP Address assigned by an ISP. What is now more typical is that one home may connect to the Internet using multiple digital devices simultaneously, including laptops, tablets, smart phones, smart televisions, and gaming systems, by way of example. Because the home subscriber typically only has one Internet connection and is only assigned one IP Address at a time by their ISP, multiple devices in a home are connected to the Internet via a router or hub. Internet activity from every device attached to the router or hub is utilizing the same external IP Address assigned by the ISP. The router or hub "routes" Internet traffic so that it reaches the proper device. Most ISPs control a range of IP Addresses. The IP Address for a user may be relatively static, meaning it is assigned to the same subscriber for long periods of time, or dynamic, meaning that the IP Address is only assigned for the duration of that online session. Most ISPs maintain records of which subscriber was assigned which IP Address during an online session.

f. IP Address -- IPv6. Due to the limited number of available IPv4 IP addresses, a new protocol was established using the hexadecimal system to increase the number of unique IP addresses. An IPv6 consists of eight sets of combination of four numbers 0-9 and/or letters A through F. An example of an IPv6 IP address is 2001:0db8:0000:0000:0000:ff00:0042:8329.

g. The following definitions:

i. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally

short to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

ii. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit links to electronic files to other individuals within the chat room.

iii. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

iv. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where: (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

v. "Cloud-based storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is typically free and readily available to anyone who has an Internet connection.

vi. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. See 18 U.S.C. § 1030(e)(1).

vii. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data.

Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

viii. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

ix. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which

perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

x. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

xi. "Encryption" is the process of converting data into a code to prevent unauthorized access to the data.

xii. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

xiii. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

xiv. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device

to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most ISPs control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

xv. "Log files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

xvi. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

xvii. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices

that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

xviii. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

xix. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

xx. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

xxi. A "storage medium" or "storage device" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

xxii. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been

transmitted by any means, whether or not stored in a permanent format.

xxiii. A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

VI. TRAINING AND EXPERIENCE ON INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

12. Based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who view and possess multiple images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or in other visual media, or from literature describing such activity. These individuals often maintain possession of these items for long periods of time and keep their collections in numerous places -- in digital devices in their homes, in their cars, in their workplaces, or on their persons.

b. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials (including through digital distribution via the Internet); conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. These individuals often maintain possession of these items for long periods of time.

13. Digital child pornography on a digital device is easy to maintain for long periods of time. Modern digital devices often have extremely large storage capacities. Furthermore, cheap and readily available storage devices, such as thumb drives, external hard drives, and compact discs make it simple for individuals with a sexual interest in children to download child pornography from the Internet and save it -- simply and securely -- so it can be accessed or viewed indefinitely.

14. Furthermore, even if a person deleted any images of child pornography that may have been possessed or distributed, there is still probable cause to believe that there will be evidence of the illegal activities -- that is, the possession, receipt, and/or distribution of child pornography -- on any digital device on WHITE's person. Based on my training and experience, as well as my conversations with digital forensic experts, I know that remnants of such files can be recovered months or years after they have been deleted from a computer

device. Evidence that child pornography files were downloaded and viewed can also be recovered, even after the files themselves have been deleted, using forensic tools. Because remnants of the possession, distribution, and viewing of child pornography is recoverable after long periods of time, searching WHITE's person could lead to evidence of the child exploitation offenses.

VII. CHARACTERISTICS OF PARTICIPANTS SUCH AS WHITE

15. Based on my training and experience, it is common for adult males who participate in sexually explicit conversations with minors using social media to also do the following:

a. Participate in sexually explicit conversations with multiple minor victims at the same time.

b. Participate in a period of grooming with these victims initially to entice production of child pornography later in the conversation.

c. To maintain a library of sexually explicit images on their electronic devices for use during these conversations.

d. To collect child pornography videos and images because of their sexual attraction to minors.

VIII. STATEMENT OF PROBABLE CAUSE

A. January 27, 2022: DACID Receives a Tip Regarding WHITE Having an Inappropriate Sexual Relationship with a 14-Year-Old (E.V.G.)

16. Based on my conversations with DACID Special Agent Caitlin A. McCay and review of her notes and reports, I know that on or about January 27, 2022, she received a call from Deputy Jacob Roberts ("Deputy Roberts") from the Bay County

Sheriff's Office in Panama City, Florida. During this call, Deputy Roberts told Special Agent McCay that WHITE, then a 21-year-old private in the United States Army stationed at Fort Irwin, had been exchanging sexually explicit photographs and videos with E.V.G., a 14-year-old who, at the time, lived in Florida. Deputy Roberts also stated that during a forensic interview, on or about that same date, E.V.G. purported to be in a relationship with WHITE. According to E.V.G., WHITE knew that s/he was 14 years old, and when they first met via Instagram, WHITE presented himself as a 15-year-old boy.

17. According to Special Agent McCay, Deputy Roberts first learned that WHITE was in contact with E.V.G. via the Florida Department of Children and Families ("DCF"), who presented the Bay County Sheriff's Office with the allegation that WHITE was engaging in a sexual relationship with E.V.G., a minor. After learning that WHITE was in contact with E.V.G., Deputy Roberts conducted a forensic interview of E.V.G. with a DCF Child Protective Investigator (Carlos Torres) and E.V.G.'s caregiver (S.D.) also present.

18. Based on my conversations with Special Agent McCay and review of her notes and reports, I also know that during their January 27, 2022 phone conversation, Deputy Roberts stated that during the forensic interview, he asked E.V.G. if he could review and use his/her phone. E.V.G. said that he could. When reviewing E.V.G.'s phone, Deputy Roberts found messages between E.V.G. and a Snapchat user called "panda4985," who had the vanity name "Hubby." Upon reviewing these messages, Deputy

Roberts saw photographs of a white male in a United States Army uniform. Deputy Roberts continued to review messages between E.V.G. and WHITE and saw that E.V.G. called WHITE, "Dada," and that WHITE called E.V.G., "Baby." In messages, WHITE also referenced their four-month anniversary and told E.V.G., "don't think you getting dick tonight either." Then, acting in an undercover capacity, Deputy Roberts used E.V.G.'s phone and posed as him/her to converse with WHITE. Deputy Roberts, acting as E.V.G., messaged WHITE and told him that DCF was at his/her home again. WHITE responded, "so no tease right now." Deputy Roberts responded that WHITE could "tease," and WHITE replied by sending two photographs of his penis. Deputy Roberts continued to communicate with WHITE, who in response, sent two videos of him lying in a barracks bed masturbating as well as a photograph of his face. In the video and photographs, WHITE appeared to be wearing a United States Army uniform.

19. Based on my conversations with Special Agent McCay and review of her notes and reports, about or around 1:15 p.m., on or about January 27, 2022, Deputy Roberts sent Special Agent McCay screenshots and videos of the conversation that he had, while acting in an undercover capacity, with WHITE via Snapchat. I later reviewed these videos and photographs.

B. January 27, 2022: DACID Conducts a Mirandized Interview of WHITE During Which He Admits to Having a Sexual Relationship with E.V.G.

20. Based on my conversations with Special Agent McCay and review of her notes and reports, around or about 5:56 p.m., on or about January 27, 2022, Special Agent McCay interviewed

WHITE. Special Agent McCay advised WHITE of his Miranda rights. WHITE waived his Miranda rights and agreed to participate in an interview. This interview, including WHITE's Miranda waiver, was recorded, and I have reviewed the recording. My knowledge of the substance of this interview is, therefore, also based upon my review of the recording. During the interview, WHITE admitted to being in a relationship with E.V.G. and to sending him/her nude photographs and videos. WHITE stated that he met E.V.G. through an ex-partner of his, who was friends with E.V.G. on Instagram, and that he and E.V.G. had been dating since September 2021. WHITE admitted that he knew E.V.G. was 14 years old and claimed that he was trying to help him/her because s/he was a victim of sexual abuse. WHITE stated that he and E.V.G. communicated via Snapchat and text, and that many of these conversations were reciprocally sexual in nature. WHITE admitted he had been sending E.V.G. nude photographs and videos since October 2021. WHITE admitted that E.V.G. would send him nude videos and photographs and that he would masturbate to them. WHITE stated that he accidentally saved one of E.V.G.'s masturbation videos on his phone, which depicted him/her masturbating with a hairbrush. WHITE stated he had about five or six romantic partners who were minors, but he could only remember one of their names. WHITE then mentioned one partner (M.T.) who was 17 when they began dating but had recently turned 18 years old. WHITE stated that he would meet random minors by using the "quick add" function on Snapchat. WHITE stated that E.V.G. was the only minor who sent him photographs and videos.

C. January 27, 2022: DACID Reviews SUBJECT DEVICE 1 and Finds Approximately 27 Photographs and Videos Containing Suspected Child Pornography

21. Based on my conversations with Special Agent McCay and review of her notes and reports, about or around 4:06 p.m., on or about January 27, 2022, Military Magistrate Jessica W. Ma provided Magistrate Authorization[1] to seize and review WHITE's cellphone (SUBECT DEVICE 1). Pursuant to that authorization, Special Agent McCay collected SUBJECT DEVICE 1 from him on or about January 27, 2022, and, following a cellphone extraction, conducted a review on or about February 22, 2022. Pursuant to her review, Special Agent McCay discovered approximately 27 photographs and videos of suspected child pornography, including nude and semi-nude photographs of E.V.G., and a video of E.V.G. masturbating with a hairbrush. The video showed only the vaginal area of the individual (E.V.G.) who was masturbating with a red hairbrush.

22. Based on my conversations with Special Agent McCay and review of her notes and reports, Special Agent McCay also reviewed text messages and Instagram chats between WHITE and presumed minors. WHITE would generally message the minors and tell them that they were beautiful and that he would treat them like "queens." Based on my training and experience, I believe that WHITE engaged in a practice called "grooming," which consists of befriending and establishing an emotional connection

[1] DACID utilize Military Magistrates to provide authorization for the search and seizure of any property, located on a military installation. See Army Regulation 27-10, Chapter 8, Section III.

with a minor to lower the child's inhibitions with the objective of initiating a sexual relationship. WHITE would typically ask their age, and if they stated that they were under 18, he would, nevertheless, continue communicating with them. Of note, Special Agent McCay found communications between WHITE and C.D. (an acquaintance or relative of E.V.G.'s) that occurred on or about November 30, 2021. In these communications, WHITE told C.D. to "paddle" E.V.G. if she misbehaved. In conversations with C.D., on or about November 15, 2021, WHITE also stated that he had numerous punishments for E.V.G. if s/he misbehaved, and he described himself as a "dom."[2]

D. May 11, 2022 and June 6, 2022: DACID Attempts to Identify Additional Minor Victims

23. On or about May 11, 2022, I copied suspected child pornography materials from SUBJECT DEVICE 1 and placed them on a USB, which I then mailed to National Center for Missing and Exploited Children ("NCEMEC"), for examination and identification of unknown minor victims. NCMEC has not yet identified the individuals in the submitted images.

24. On or about June 6, 2022, I reviewed WHITE's Snapchat records and saw sexually explicit photographs and videos of what I believed to be minors. I was able to identify the following individuals and confirm, through law enforcement databases, that they were indeed minors: L.M., C.W., H.S., and R.S. I also found photographs and videos on Snapchat from a suspected minor

[2] Based on my training and experience, I know that "dom" is a term commonly used in Bondage, Discipline, Domination and Sadism ("BDSM") culture. In BDSM culture, a "dom" is someone who exercises control over their submissive partner.

using the username "thekilling420;" however, I was unable to identify him/her at the time.

E. June 7, 2022: DACID Conducts a Second Mirandized Interview with WHITE During Which He Admits to Remaining in Contact with Suspected Minors and Possessing Suspected Child Pornography

25. Based on my conversations with Special Agent McCay and review of her notes and reports, on or about June 7, 2022, Special Agent McCay interviewed WHITE. Special Agent McCay advised WHITE of his Miranda rights. WHITE waived his Miranda rights and agreed to participate in an interview. This interview, including WHITE's Miranda waiver, was recorded, and I have reviewed the recording. My knowledge of the substance of this interview is, therefore, also based upon my review of the recording. During the interview, WHITE admitted that he was still contacting presumed minors using his cellphone. WHITE admitted that he continued to receive sexually explicit photographs and videos from these presumed minors. WHITE stated that he had updated his new cellphone, using iCloud, to download the child pornography that was on SUBJECT DEVICE 1 (the phone that DACID had seized on or about January 27, 2022). WHITE stated that he understood his cellphone had been seized by DACID because he could access his iCloud from his phone, and then he proclaimed, "you realize I can get into it from any fucking computer on base. It's not that fucking hard."

26. Prior to this interview, on or about June 7, 2022, Military Magistrate Gunnar Carroll provided Military Authorization for DACID to seize and review WHITE's second

cellphone (SUBJECT DEVICE 2). Pursuant to that authorization, I seized and reviewed SUBEJCT DEVICE 2, and I found the same photographs and videos that were on SUBJECT DEVICE 1. I did not find any new photographs or videos of suspected minors either nude, semi-nude, or engaging in sexually explicit acts.

F. August 15, 2022: DACID Identifies Another Minor Victim (E.B.)

27. On or about August 15, 2022, I discovered, from Snapchat records, that the profile "thekilling420" was associated with E.B. On or about September 7, 2022, I contacted E.B. via the telephone and asked what his/her age was. E.B. stated that s/he was 16. I then asked him/her to provide contact information for his/her parent or guardian. E.B. gave me the phone number of his/her parent, M.B.

28. On or about September 7, 2022, I spoke with M.B. via the phone. During this conversation s/he stated that his/her child (M.B.) was 16 years old and used the username "thekilling420" on Snapchat. M.B. declined to allow DACID to interview E.B.

IX. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[3]

29. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I

[3] As used herein, the term "digital device" includes the SUBJECT DEVICES and any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners,

(footnote cont'd on next page)

know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat

---

monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

30. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it can take a substantial period of time to search digital devices and it is not always possible to search devices for data during a search of a premises or person for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so

many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

31. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after

a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress WHITE's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of WHITE's face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature.

32. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

//

//

//

//

//

//

//

//

//

//

//

//

X. CONCLUSION

33. For all the reasons described above, there is probable cause to believe WHITE has committed a violation of 18 U.S.C. § 1470 (Transfer of Obscene Material to a Minor). There is also probable cause that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICES and the person described in Attachments A-1 and A-2.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 21st day of February, 2023.

MARGO A. ROCCONI
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

PROPERTY TO BE SEARCHED

The following digital devices (collectively, the "SUBJECT DEVICES"):

1. a Black iPhone SE, Model MMX53LL/A, bearing IMEI No. 350472506112686, and bearing Serial No. NMMW69595K seized on or about January 27, 2022, and currently maintained in the custody of Department of the Army Criminal Investigation Division ("DACID") in Fort Irwin, California ("SUBJECT DEVICE 1"); and

2. a Black/Grey iPhone 12 Pro Max, Model MG923LL/A, bearing IMEI No. 354876506002091, and bearing Serial No. F2LF69170D43 seized on or about June 7, 2022, and currently maintained in the custody of DACID in Fort Irwin, California ("SUBJECT DEVICE 2").

ATTACHMENT A-2

PERSON TO BE SEARCHED

The person of PARKER WILLIAM WHITE ("WHITE"), date of birth 10/2/2000, based on biographical data collected from WHITE by the Department of the Army Criminal Investigation Division (DACID), he is known to stand at 5'8" tall and weigh 207 pounds with black hair and hazel eyes.

The search of WHITE shall include any and all clothing and personal belongings, digital devices, backpacks, wallets, briefcases, purses, and bags that are within WHITE's immediate vicinity and control at the location where the search warrant is executed.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 2251(Sexual Exploitation of Children); 18 U.S.C. § 2252A (Certain Activities Relating to Material Constituting or Containing Child Pornography); 18 U.S.C. § 2422(b) (Coercion and Enticement of a Minor to Engage in Criminal Sexual Activity); and 18 U.S.C. § 1470 (Transfer of Obscene Material to a Minor) (the "SUBJECT OFFENSES"), namely:

a. Child pornography, as defined in 18 U.S.C. § 2256(8);

b. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer to child pornography, as defined in 18 U.S.C. § 2256(8), including but not limited to documents that refer to the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography;

c. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer or relate to any production, receipt, shipment, order, request, trade, purchase, or transaction of any kind involving the transmission through interstate commerce by any means, including by computer, of any visual depiction of a minor

engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

d. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, identifying persons transmitting in interstate commerce, including by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

e. Any and all records, documents, programs, applications, or materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings;

f. Records, correspondence, financial information, receipts, wire transfer records, airline ticket information, records of searches on the Internet, and visual depictions, as that term is defined in Title 18, United States Code, Section 2256, regarding travel by WHITE from California to Florida from about or around September 2021 to present.

g. As used above, the terms records, correspondence, financial information, receipts, wire transfer records, airline ticket information, records of searches on the Internet, and

visual depictions, includes records, correspondence, financial information, receipts, wire transfer records, airline ticket information, records of searches on the Internet, and visual depictions created, modified or stored in any form including electronically.

h. Any records, documents, programs, applications, or materials identifying possible minor victims depicted in child pornography and/or minor victims of sexual abuse;

i. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, which pertain to the Instagram Application;

j. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, which pertain to accounts with any Internet Service Provider;

k. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, regarding ownership and/or possession of the SUBJECT DEVICES or any other digital device on WHITE's person and within WHITE's immediate vicinity and control at the location where the search warrant is executed;

l. Any records, documents, programs, applications, or materials, including images and/or videos, of WHITE's naked body or other sexual content sent to persons who appear to be minors under the age of 18;

m. Any records, documents, programs, applications, or materials of communication between WHITE and any person who

appears to be a minor under the age of 18 that involve the discussion of sexual activities;

n. Records, documents, programs, applications, materials, and files relating to the deletion, uploading, and/or acquisition of victim files to include photographs, videos, e-mails, chat logs, or other files;

o. Records, documents, programs, applications, materials, and files relating to the online social media accounts of any victim; and

p. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

q. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes the SUBJECT DEVICES and any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet

computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the scope of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques, including to search for known images of child pornography.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the scope of items to be seized, the government will, as soon as is practicable,

return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the scope of items to be seized, the government may make and retain copies of such data and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the scope of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to

law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. During the execution of this search warrant, law enforcement is permitted to: (1) depress WHITE's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of WHITE's face with his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.